UNIVERSIDADE DA AMAZÔNIA – UNAMA
CENTRO DE CIENCIAS EXATAS E DE TECNOLOGIA – CCET
Cursos de Computação e Informática – CCI
Curso de Bacharelado em Ciência da Computação

CARLOS ALBERTO DE CARVALHO VAZ PEREIRA JUNIOR
GUSTAVO DA SILVA BRABO
ROMULO AUGUSTO DE SALES AMORAS

SEGURANÇA EM REDES WIRELESS PADRÃO IEEE802.11b: PROTOCOLOS WEP, WPA E ANÁLISE DE DESEMPENHO

Trabalho de Conclusão de Curso apresentado, como requisito parcial para obtenção de do Grau de Bacharel em Ciência da Computação, à Universidade da Amazônia, sob orientação da Prof$^{\underline{a}}$. M.Sc. Thienne M. Johnson.

Belém/PA
2004

UNIVERSIDADE DA AMAZÔNIA – UNAMA
CENTRO DE CIENCIAS EXATAS E DE TECNOLOGIA – CCET
Cursos de Computação e Informática – CCI
Curso de Bacharelado em Ciência da Computação

CARLOS ALBERTO DE CARVALHO VAZ PEREIRA JUNIOR
GUSTAVO DA SILVA BRABO
ROMULO AUGUSTO DE SALES AMORAS

SEGURANÇA EM REDES WIRELESS PADRÃO IEEE802.11b: PROTOCOLOS WEP, WPA E ANÁLISE DE DESEMPENHO

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de do Grau de Bacharel em Ciência da Computação, à Universidade da Amazônia, sob orientação da Prof[a] M.Sc. Thienne M. Johnson.

Data da defesa:
Conceito:

Banca Examinadora

AGRADECIMENTOS

À Deus, por iluminar nossos caminhos e nos guiar na direção certa, permitindo que vencêssemos todos os obstáculos.

À nossas famílias, pelo apoio emocional que nos permitiu o equilíbrio e tranqüilidade necessária, e pelo amor que sempre nos deram.

À nossa orientadora, Thienne Johnson, por ter depositado sua confiança em nossos esforços e pela sua competência na condução de nosso trabalho.

Ao nosso coordenador, Alex Costa, pela ajuda prestada durante a fase final de elaboração de nosso TCC, que foi de imensa importância.

À todos nossos amigos, que de alguma forma estiveram nos ajudando e dando força para realização deste trabalho.

A sabedoria consiste em compreender que o tempo

Dedicado ao trabalho nunca e perdido.

RALPH

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIAÇÕES E SIGLAS

AES - *Advanced Encryption Standard*
AP - *Acess Point* ou Ponto de Acesso
CRC - *Cyclic Redundancy Check*
CRC-32 - *Cyclic Redundancy Check 32*
CSMA-CD - *Carrier Sense Multiple Access with Collision Detection*
DoS - *Denial of Service*
DSSS - *Direct Sequence Spread Specrtum*
EAP - *Extensible Authentication Protocol*
FTP - *File Transfer Protocol*
HTTP – *Hypertext Transfer Protocol*
ICSA – *International Computer Security Association*
ICV - *Integrity Check Value*
IEEE - *Institute of Electrical and Electronics Engineers*
IFG - *Interframe Gap*
IP – *Internet Protocol*
ISM - *Industrial, Scientific, and Medical*
LAN – *Local Area Network*
LEAP - *Lightweight Extensible Authentication Protocol*
MAC - *Media Access Control*
MIC - Código de Integridade da Mensagem
NIST – *National Institute of Standards and Technology*
PRNG - *Pseudo Random Number Generator*
PSKS - *Pre-Shared Keys*
RADIUS - *Remote Authentication Dial-In User Service*
SMTP - *Simple Mail Transfer Protocol*
SNMP – *Simple Network Managment Protocol*
SSID - *Service Set Identification*
TCP – *Transmission Control Protocol*
TKIP - *Temporal Key Integrity Protocol*
VPN - *Virtual Private Network*
WEP - *Wired Equivalent Privacy*
WI-FI – *Wireless Fidelity*
WIRELESS – *Rede Sem Fio*
WLAN - Redes Locais Sem Fio
WPA - *Wired Protected Acess*

RESUMO

O presente projeto apresenta uma descrição da forma de funcionamento do padrão IEEE 802.11b, focando especificamente as características envolvendo a segurança neste tipo de ambiente. São descritos os mecanismos de segurança deste padrão e as fraquezas do protocolo de segurança WEP e WPA. Também são apresentadas algumas conclusões de experimentos práticos medindo o fluxo da rede ao utilizar este protocolos.

ABSTRACT

The current project presents a description of how the IEEE standard 802.11b works, specifically the characteristics involving security in this type of environment. The security measures of this standard are described and the weaknesses of the WEP and WPA security protocols analyzed. Also, some conclusions of practical experiments measuring the throughput of the network when using these protocols are presented.

1 INTRODUÇÃO

As redes locais sem fio vêm se tornando cada vez mais utilizadas no meio corporativo, haja vista que, o ganho na flexibilidade e na mobilidade dos equipamentos destes padrões implicam cerca de 22% (GUANDÊNCIO, 2003) na produtividade das empresas tornando esta estrutura vantajosa. Além disso, vale a pena refletir sobre conceitos colhidos em entrevistas recentes com especialistas e líderes como Carly Fiorina (da HP), John Chambers (da Cisco), Bill Gates (da Microsoft), Jean-Paul Jacob (da Universidade de Berkeley e da IBM) que focam exatamente na mudança da comunicação com fio para a sem fio (*WIRELESS*).

Apesar disso, existem restrições quanto ao seu uso, devido às diversas vulnerabilidades encontradas no padrão 802.11x. Sendo assim, há várias medidas de segurança que devem ser adotadas ao implementar este padrão, gerando a este campo uma grande importância, haja vista que os acessos indevidos a estes ambientes são freqüentes.

Há várias oportunidades de desenvolvimento de segurança para as redes WI-FI (*Wireless Fidelity*) tendo como reflexo os desenvolvimentos tanto no meio acadêmico como no meio empresarial.

O Padrão IEEE (*Institute of Electrical and Electronics Engineers*) 802.11b, tenta aplicar alguns mecanismos de segurança para que os dados que trafegam na rede possam obter sua confidencialidade e integridade desejada, sendo o WEP *(Wired Equivalent Privacy)*, o protocolo mais popular responsável pela execução

destes mecanismos no nível de enlace, gerando uma grande discussão pelos especialistas sobre sua eficiência. Como conseqüência, propostas de várias instituições são apresentadas, como a CISCO que em 2003 lançou o padrão WPA (*Wired Protected Acess*).

O WPA é o protocolo de segurança que teve como base no desenvolvimento de sua estrutura em geral os erros do protocolo WEP e assim ganhou grande proporção no mercado mundial. Devido a isto, este documento irá no terceiro capítulo abordar uma comparação entre estes dois protocolos.

Este trabalho tem por objetivo estudar em detalhes as características do padrão IEEE 802.11b, dando ênfase aos protocolos de segurança WEP e o WPA. São discutidas as principais vantagens e desvantagens de cada protocolo, tendo o respaldo de testes práticos que foram realizados entre esses protocolos, para a maior eficácia do resultado desses testes.

Propondo com os resultados dos testes realizados qual o protocolo que além de ser mais seguro trabalha de forma mais rápida no momento de criptografar os dados que estão migrando na rede.

Este trabalho está subdividido em quatro capítulos. Na primeira parte apresenta-se um resumo do tema, a parte introdutória, visão do cenário escolhido e qual o objetivo deste trabalho.

No segundo capítulo descreve-se os conceitos e as principais características do padrão 802.11b, juntamente com uma análise sobre os

mecanismos de invasão mais freqüentes e suas principais técnicas e medidas que tornam este padrão menos vulneráveis aos ataques são descritas.

No terceiro capítulo os protocolos de criptografia WEP e WPA serão definidos detalhadamente, e será feita uma comparação entre os dois protocolos, levando em consideração a confiabilidade, integridade, autenticidade e vulnerabilidades.

Complementando esta etapa será feita uma análise da taxa de transferência e tempo de ambos os protocolos através de simulações práticas, levando em consideração o tipo de criptografia utilizado.

E por fim uma conclusão, definida pelos resultados e opiniões obtidas ao decorrer do trabalho, com uma ênfase nos testes práticos.

2 PADRÃO IEEE 802.11b

2.1 Principais Características

Existem muitos padrões de WLAN (*Wireless Local Area Network*) em uso, o mais popular até agora é o padrão IEEE 802.11b, que define um conjunto de protocolos de comunicação para uma rede sem fio em banda de freqüência ISM (*Industrial, Scientific, and Medical*) de 2.4GHz, com DSSS (*Direct Sequence Spread Specrtum*). As redes 802.11b podem operar com velocidades de até 11Mbps, podendo alcançar uma distância de 450 metros em ambientes abertos ou 50 metros em ambientes fechados. Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando, tais como paredes, vidros, ondas eletromagnéticas e interferências de um modo geral, que podem prejudicar esta propagação.

Por ser uma transmissão aberta, qualquer pessoa com um receptor operando na mesma freqüência poderá captar as ondas. Devido a isto, técnicas como o *Wardriving* (seção 2.2.7) são freqüentes neste meio. Logo, o administrador da rede terá que calcular o lugar exato para o *Ponto de acesso* (AP), para que as ondas de freqüência não ultrapassem o limite da propriedade ou ultrapassem o mínimo possível. Na tabela 2.1 mostra-se de uma forma geral as características do padrão 802.11b.

Tabela 2.1 – Características do padrão 802.11b

Característica	Descrição
Camada Física	DSSS
Freqüência	2.4 Ghz
Método De Acesso	CSMA/CD
Taxa De Transferência	11 Mbps
Propagação	50 Metros (Ambiente Fechado) 450 Metros (Ambiente Aberto)
Capacidade	11 Mbps (54 Mbps Planejados)
Prós	Grande Quantidade De Fornecedores, Preços Cada Vez Mais Baixos
Contras	Segurança Fraca, Capacidade De Trafego Pode Vir As Sofrer Um Gargalo

2.1.1 Modos de Operação

WLANS funcionam basicamente de dois modos de operação: Infraestruturado e *Ad-Hoc*.

O modo de operação infraestruturado também conhecido como “configuração de um serviço básico” (BBS), utiliza estações e *Ponto de acesso*. Uma estação é qualquer dispositivo sem fio, podendo ser *PocketPC*, seu *laptop* ou *Xbox*. Um *Ponto de acesso* é como o *hub* ou um *switch* de uma rede com fio: as estações conectam-se a ele formando uma associação (chamada de porta) com o *Ponto de acesso*.

Este modo é mostrado na figura 2.1 de uma forma simplificada. Normalmente usado em aplicações comerciais, tanto para ambientes fechados como para áreas abertas.
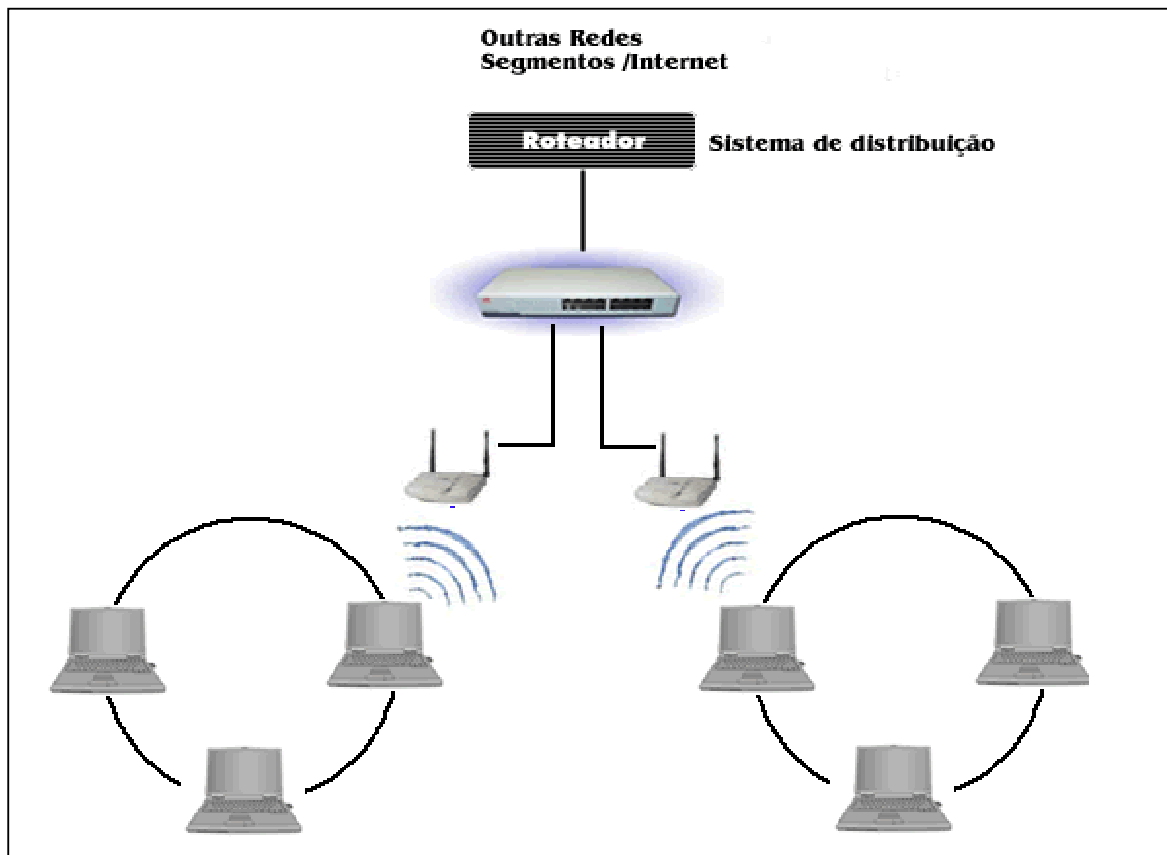
Figura 2.1 – Modo Infraestruturado

O modo de operação *ad-hoc*, também conhecido como ponto-a-ponto, em contraste, funciona com as estações conversando diretamente entre si, sem usar um *Ponto de acesso* para gerenciar a rede e oferecer serviços. Pode ser implementado usando técnicas de *broadcast* ou mestre – escravo, como mostra a figura 2.2.

Figura 2.2 – Modo *Ad – Hoc*

2.1.2 Tipos de Autenticação

O padrão IEEE 802.11b define duas formas de autenticação: *open system* e *shared key*. Independentemente da forma escolhida, toda autenticação deve ser realizada entre pares de estações, nunca havendo comunicação *multicast*. Em sistemas BBS, as estações devem se autenticar e realizar a troca de informações através do *Access Point* (ROSS, 2003).

2.1.2.1 Autenticação *Open System*

É o sistema de autenticação padrão onde qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo. A autenticação do tipo *Open System* foi desenvolvida focando redes que não necessitam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção.

2.1.2.2 Autenticação *Shared Key*

Nestas autenticações, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

A autenticação *shared key* utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. A forma de obter esta autenticação e mostrada na figura 2.3 e realizada da seguinte forma:

1 - Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o *Ponto de acesso*.

2 - O *Ponto de acesso* responde a esta requisição com um texto desafio contendo uma chave de informações pseudo-randômicas.

3 - A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para criptografar a chave enviada pelo *Ponto de acesso* e devolvendo estes dados ao *Ponto de acesso*.

4 - O *Ponto de acesso* conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a criptografia da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.
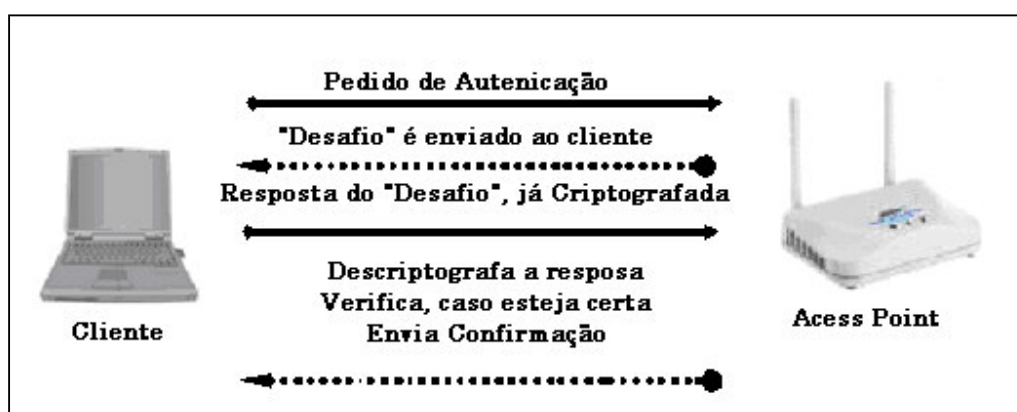
Figura 2.3 – Autenticação do cliente feita com "Shared Key"

Ambos os métodos são antigos e extremamente vulneráveis. Outro problema é que, para fazer com que as redes sem fio possam ser colocadas em funcionamento com rapidez, os mecanismos de segurança existentes nos equipamentos costumam vir desabilitados, isso quando existem.

Este é o problema principal das redes sem fio: 80% delas não usam nem mesmo os mecanismos básicos de segurança, de acordo com as pesquisas feitas em 2003 pela CISCO. O pouco entendimento sobre arquitetura de redes faz com que o profissional não entenda exatamente como a rede sem fio funciona e como ela se encaixa no ambiente já existente. Uma boa ou má implementação de rede sem fio na corporação poderá fazer a diferença entre riscos gerenciáveis e riscos inaceitáveis.

Por exemplo, não é trivial especificar com exatidão qual é o alcance de redes wireless. De acordo com o *paper Wireless Network Security* do NIST (*National Institute of Standards and Technologies*), devido às diferenças entre construções de prédios, freqüências, atenuações e antenas de alta potência, a distância correta de propagação pode variar consideravelmente, mesmo que às especificações mencione poucos metros.

Nas redes com fio existem um, ou alguns pontos de acesso à sua rede, porém em redes wireless, qualquer ponto localizado em uma distancia aproximada entre 50 a 450metros pode ser um acesso em potencial. Por isso o uso de técnicas de detecção de *Access Points* não autorizados na rede é imprescindível.

Durante a conferencia *hacker* Defcon X, ocorrida em agosto de 2002 em Las Vegas, foram detectados mais de 10 novos tipos de ataques, segundo a AirDefense. Uma parte preocupante revelou ataques mais sofisticados que exploram falhas no protocolo 802.11b, o que mostra que os *hackers* estão se aprofundando cada vez mais no padrão.

2.1.3 Ssid – Service Set Id

O SSID (*Service Set Identification*) é um conjunto de caracteres alfanuméricos que identifica uma rede *wireless*. A maioria dos dispositivos sem fios vem com o SSID *broadcast* ativado por *default*, de forma a que, durante a implementação, se torne muito mais fácil a localização dos pontos de acesso. Após o processo de implementação, deverá ser desativado o SSID *broadcast* nos pontos de acesso, de modo a proteger os acessos "estranhos", permitindo a entrada apenas aos utilizadores que conhecem o SSID válido.

Caso o sistema de criptografia não estiver ativo, o SSID também funciona como uma senha para usuários não autorizados, pois a autenticação ao ponto de acesso só será permitida se o usuário souber os caracteres exatos que identificam a rede para poder ter acesso e usufruir as informações disponíveis na rede.

Na situação em que o SSID por algum motivo modificar em sua configuração, todos os integrantes terão que sofrer atualizações para continuarem permanecendo na rede.

2.1.4 Método Utilizado para o Controlar o Acesso ao Meio Físico

Mais especificamente, a subcamada MAC (*Media Access Control*) do 802.11b oferece, em uma configuração com infraestrutura, um método centralizado de controle de acesso baseado em consulta, onde os pontos de

acesso são responsáveis pela alocação de banda passante e pela limitação da latência das estações.

O desempenho deste modo de acesso está diretamente ligado aos algoritmos de consulta utilizados, os quais buscam um compromisso entre a eficiência na utilização da banda passante e a capacidade em oferecer garantias estritas de desempenho aos tráfegos sensíveis ao tempo.

O método de acesso ao meio físico (MAC) é o protocolo CSMA-CD (*Carrier Sense Multiple Access with Collision Detection*), que trabalha da seguinte forma:

a) *Carrier sense*: a estação que precisa transmitir um pacote de informação tem que se assegurar de que não há outros nós ou estações utilizando o meio físico compartilhado antes de iniciar a transmissão.

b) Se o canal estiver livre por um certo período de tempo, denominado IFG (*Interframe Gap*), a estação pode iniciar a transmissão.

c) Se o canal estiver ocupado, ele será monitorado continuamente até ficar livre por um período de tempo mínimo de IFG, então a transmissão é iniciada.

d) Quando duas estações ou mais detectam que o canal esta livre e iniciam a transmissão ao mesmo tempo, ocorre a colisão, que destrói os pacote de dados enviados.

O MAC Ethernet monitora continuamente o canal durante uma transmissão para detectar essas colisões. Se uma estação identifica uma colisão durante a

transmissão, esta é imediatamente interrompida e um sinal de congestionamento (JAM) é enviado ao canal para garantir que todas as estações identifiquem a colisão e rejeitem qualquer pacote de dados que possam estar recebendo, para não haver erros.

e) Após um período de espera (*backoff*), nova tentativa de transmissão é feita pelas estações que precisam transmitir. Um algoritmo de *backoff* determina um atraso de modo que diferentes estações tenham que esperar tempos diferentes antes que nova tentativa de transmissão seja feita.

Um detalhe é que o CSMA/CD é o mesmo utilizado nas redes *Ethernet*, sendo que este protocolo é usado não apenas para evitar estas colisões como descrito, vai além, chegando a ter um controle total destas colisões. Em redes sem fio a tentativa se resume apenas que estas colisões não ocorram (AUGUSTO, 2003).

2.2 Mecanismos de Invasão mais Freqüentes no Ambiente

Uma das vantagens das redes sem fio é a facilidade na hora da implementação. Com isto, o usuário, querendo fazer com que a rede funcione com rapidez, acaba não dando atenção aos mecanismos de segurança básicos, cujos fabricantes desabilitam para que o usuário tenha menos esforço ao implementar.

Um *Cracker* ou um *Hacker*, índividuo que consegue um acesso não autorizado a um computador, podendo comprometer a disponibilidade do sistema

ou da integridade ou a confiabilidade dos dados, muitas vezes não tem dificuldade em enxergar os dados de uma empresa. Estes intrusos podem ter quatro comportamentos diferentes em relação às posições de origem e destino da mensagem.

- Interrupção: sendo o principal objetivo interromper o fluxo que parte da origem, para que não chegue em seu destino como mostra a figura 2.4.
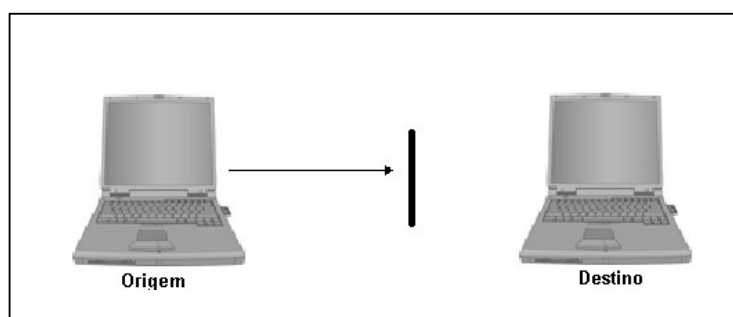
Figura 2.4 – Ataque em forma de Interrupção

- Interseção: No qual o intruso objetiva apenas tomar conhecimento das informações que trafegam na rede, como na figura 2.5.
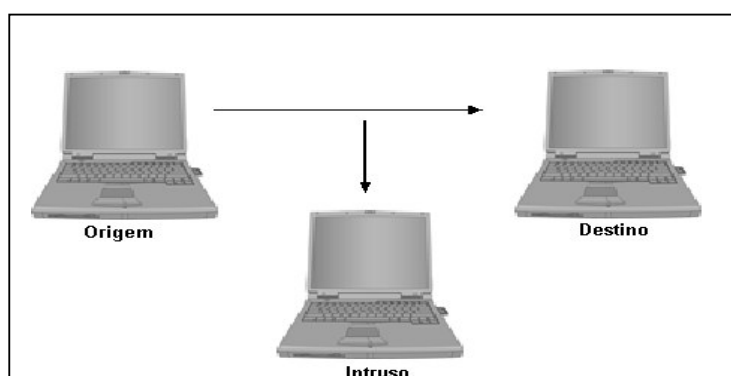
Figura 2.5 – Ataque em forma de Interseção

- Modificação: Além de "escutar" o tráfego, o intruso modifica os dados e depois envia para o destino, como na figura 2.6.
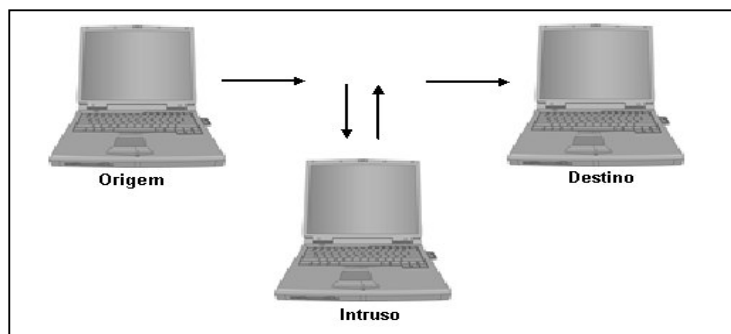
Figura 2.6 – Ataque em forma de Modificação

- Fabricação: Neste o intruso fabrica os dados e depois envia para o destino, como na figura 2.7.
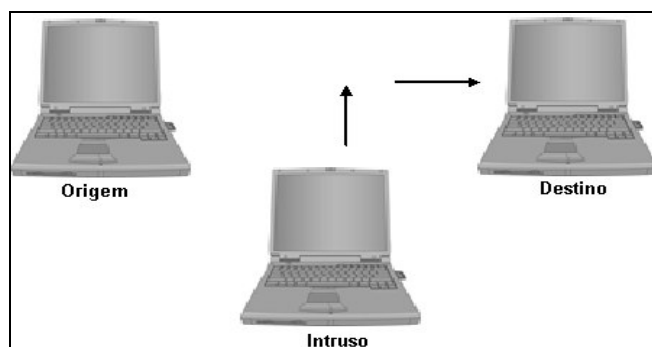
Figura 2.7 – Ataque em forma de Fabricação

É possível que um atacante obtenha todas as informações que trafegam na rede sem criptografia simplesmente capturando as informações da rede ou tendo o SSID. Mesmo na utilização de criptografia o invasor pode passar-se por um elemento da rede e assim todos os dispositivos de segurança passam a ter

confiança no invasor e, assim, não dando nenhuma dificuldade ao elemento na hora da obtenção das informações.

As próximas seções mostram várias técnicas utilizadas pelos invasores, como por exemplo, como conseguem obter as informações da rede (SSID), como quebram o sistema de criptografia, como duplicam o MAC, o mecanismo *Denial of Service* (DoS), técnicas que usam *Sniffers* e *Scanners* e o famoso *wardriving*.

2.2.1 *Denial of Service* (DoS)

Este mecanismo de ataque tenta explorar a freqüência na qual o padrão 802.11b trabalha. Como vários dispositivos trabalham com a freqüência de 2.4 GHz, estes equipamentos acabam degradando o sinal fazendo com que o rendimento da rede seja reduzida. Um usuário com intenções maliciosas e com equipamentos adequados pode simplesmente usar este artifício para derrubar o ponto de acesso. Ou seja, pode mandar uma grande quantidade de sinais na mesma freqüência com a tentativa de fazer com que a rede pare de funcionar.

Isso também pode ocorrer de forma não intencional com redes vizinhas: geralmente o mesmo fabricante utiliza o mesmo canal *default* para os mesmo equipamentos fabricados, sendo assim pode ocorrer que uma rede cause DoS na outra através da interferência de rádio.

A melhor forma de evitar ataques intencionais e não intencionais é fazer uma barreira física no ponto de acesso procurando reduzir os riscos de ruídos

externos como de eletros-domésticos que trabalham na mesma freqüência e assim trazer um melhor rendimento para a rede.

2.2.2 Scanners

Este mecanismo é um dos maiores problemas que o padrão enfrenta, pois é da característica das WLANS enviar pacotes em todas as direções para facilitar que um usuário se conecte a rede de forma mais prática. Um administrador de rede pode simplesmente desabilitar este recurso, fazendo que o ponto de acesso não envie pacotes em *Broadcast*. Mesmo assim, *softwares* como o *NetStumbler*[1] conseguem detectar a rede, pois o próprio programa envia pacotes em todas as direções, tentando desta forma localizar o ponto de acesso.

Com o intruso sabendo onde está localizado o ponto de acesso ele irá passar pra uma nova etapa caso queira realmente obter acesso a rede. A partir de então, o intruso tentará, dependendo de como a rede está protegida, conseguir um MAC válido tentando assim enganar todos os mecanismos de segurança da rede ou tentar descobrir qual seria a chave para a quebra do algoritmo de criptografia.

Primeiramente, para tentar evitar que *scanners* detectem a rede é preciso alterar o SSID *default* e, além disso, diferenciar de qualquer nome que esteja associado à empresa, pois o novo dispositivo terá que saber previamente qual é este nome, para assim, se juntar ao resto dos dispositivos. Além disso, é preciso

[1] www.netstumbler.com

desabilitar o SSID *broadcast* no ponto de acesso. A figura 2.8 mostra a interface do *NetStumbler* , funciona com sondagem ativa para tentar encontrar os pontos de acesso e levantar informações a seu respeito.
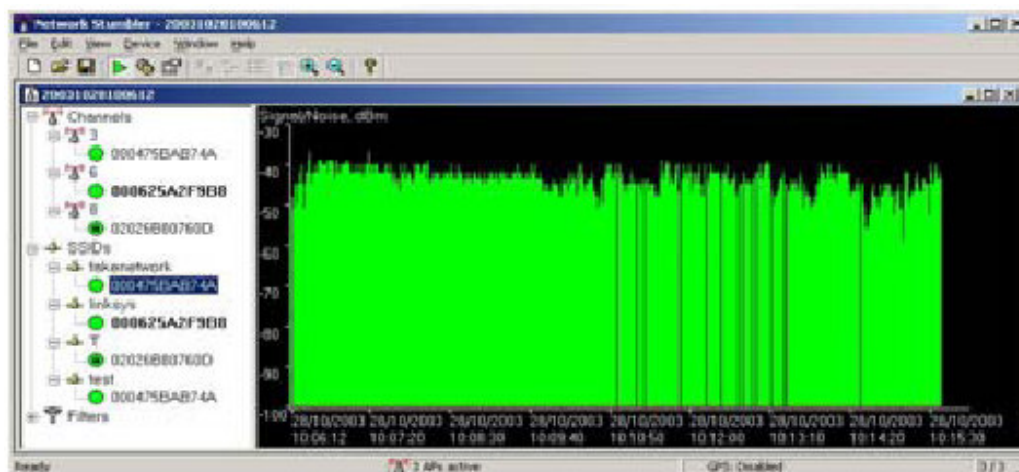
Figura 2.8 – Interface do *NetSumber*

Além de ser utilizado para ações maliciosas, pode ser utilizado pelo gerente da rede em questão, para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição. Apesar de todas as inovações trazidas por este programa, a base de sua concepção também é à base de seu maior problema. Utilizando o método de sondagem ativa da rede, suas primeiras versões enviavam informações que facilitavam a identificação destes *softwares* através da análise do tráfego da rede.

2.2.3 Mac Spoofing

Como o MAC *Address* das placas são globais, ou seja, cada uma no mundo possue a sua própria numeração, em muitos casos o administrador de rede define isto como um fator determinante para a autenticação de um usuário na rede. Isto pode não funcionar com intrusos habilidosos, pois é possível que o invasor mude seu MAC *Address* para driblar as listas de controles de acessos e assim obter privilégios na rede.

Após as vítimas se autenticarem com sucesso e passarem pela lista de *Address* MAC autorizados no ponto de acesso, o intruso pode estar monitorando neste instante a rede e assim obter uma lista de endereços MAC autorizados para se comunicar. Com a lista, o invasor só precisa alterar o seu próprio endereço MAC e assim driblar o mecanismo de segurança pretendido.

Usando a plataforma *Linux*[1] esta mudança é possível com o comando *ifconfig* ou no *Windows*[2] chamando as propriedades de seus cartões WLANS no painel de controle levando em consideração que, a maioria dos fabricantes destes cartões permite a alteração do MAC *Address* na rede (Joshua Wright, 2003).

---

[1] www.linux.org

[2] www.microsoft.com

2.2.4 Sniffers

Este mecanismo funciona basicamente como os Scanners tendo um detalhe a mais: os *sniffers*, além de tentar captar a rede e o seu ponto de acesso, também tentam fazer um armazenamento dos dados privilegiados que a empresa possue. Caso estes dados estejam criptografados, o invasor terá o trabalho de, posteriormente, tentar quebrar este algoritmo de criptografia. Caso não esteja, o índividuo não terá mais nenhuma dificuldade no entendimento da informação.

Umas das ferramentas mais famosas neste tipo de ataque é o *Kismet*[1] que também não deixa de ser um Scanner, que faz uma análise nos dados que possuem criptografia mais fraca para facilitar ao índividuo na tentativa de decifrar os dados. Outros softwares são o *Ethereal*[2] e o *TcpDump*[3].

2.2.5 Associação Maliciosa

É definida associação maliciosa quando o invasor simula um ponto de acesso através de um software chamado *softAP*[4], fazendo com que o usuário pense que está se conectando em uma rede real mas na verdade está sendo enganado.

---

[1] www.kismetwireless.net
[2] www.ethereal.com
[3] www.tcpdump.org
[4] www.softap.com

A associação entre a vítima e o atacante será mostrada na figura 2.9, a seguir:
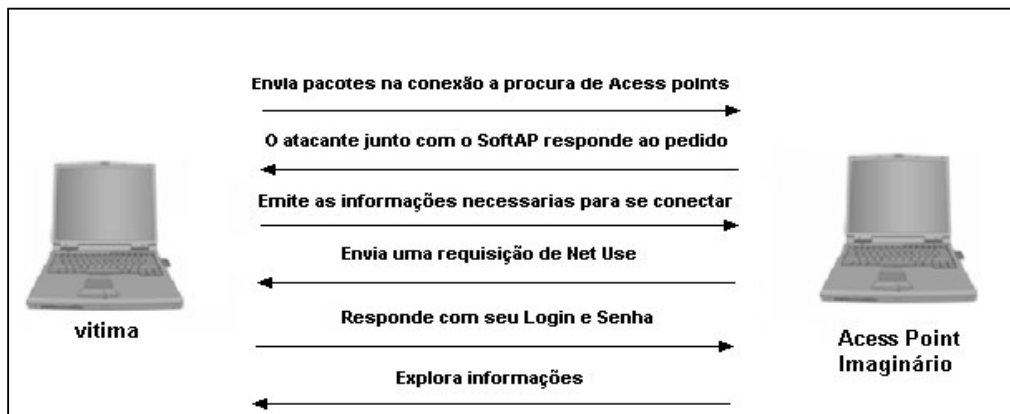
Figura 2.9 – Associação maliciosa entre vitima e atacante

2.2.6 Wardriving

Consiste em uma técnica que o invasor anda no seu carro com seu *laptop* e com uma antena tentando detectar as WLANS, definindo a onde está localizada uma rede sem fio e se é possível determinar seu nível de segurança, ou seja, se possue WEP e se está aberta ou fechada e assim tentar posteriormente invadi-la.

Posteriormente são definidos alguns destes termos para as WLAN's, dependendo de sua característica. O invasor resume seu nível de segurança da seguinte forma:

Figura 2.10 – Rede Sem Fio Aberta

Figura 2.11 – Rede Sem Fio Fechada Através do SSID

Figura 2.12 – Rede Sem Fio Fechada Através do SSID e o WEP

2.2.7 Falhas no Sistema de Criptografia WEP

Um funcionário da Intel chamado Jesse Walker foi um dos primeiros a publicamente mostrar que o algoritmo de criptografia possue falhas em seu mecanismo de funcionamento. Em uma pesquisa feita por Nikita Borisov, pesquisadora Russa, foi possível quebrar o sistema em 4 horas, utilizando 250 computadores.

A ferramenta mais famosa para este tipo de ataque que tenta fazer a quebra das chaves WEP é a *AirSnort*[1], que primeiramente captura o tráfego dos pacotes para por fim analisar. Depois que foi feito à captura suficientes destes pacotes, cerca de 1500, é iniciado o processo de quebra.

A maior motivação para que haja este tipo de *software* é o fato do Protocolo WEP utilizar a cada frame enviado um vetor de inicialização, vetor que protege a chave secreta, e assim a possibilidade de possuir o mesmo valor várias vezes é grande.

Este tópico será abordado com mais clareza no terceiro capítulo deste trabalho.

2.3 Mecanismos de Segurança

Infelizmente, um fator fundamental vem sendo colocado em segundo plano na implementação dessas redes: a segurança da informação. No meio coorporativo, o uso de uma política de segurança eficaz é imprescindível, pois há a necessidade de diminuir as vulnerabilidades e os acessos indevidos à rede.

As soluções disponíveis no mercado utilizam em sua maioria o padrão WEP para garantia de sigilo das informações. O WEP que utiliza a implementação do protocolo RC4 para realizar criptografia, já mostrou sinais de falhas graves. Pesquisadores descobriram que era possível ter acesso à chave utilizada na

---

[1] www.sourceforge.net/projects/airsnort

criptografia provocando o surgimento de diversas ferramentas para quebra do WEP na Internet.

Contar com o WEP, que está disponível na maior parte dos equipamentos wireless, está longe de ser garantia para a segurança dos dados transmitidos.

Além do WEP, não se pode dispor das demais características de segurança disponíveis em pontos de acesso e interfaces de rede. Controle de acesso por endereços MAC e comunidades SNMP são alguns exemplos de funcionalidades que podem ser burladas. E isso não é suficiente.

Para se obter um nível de segurança satisfatório é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis.

2.3.1 Análise do Ambiente

Em ambientes privados é necessário analisar a posição ideal do ponto de acesso e das antenas, para constatar que a rede poderá ou não ser acessada fora do alcance da corporação. Existem ferramentas de análise do sinal, que identifica este alcance, o *Netstumber*, já mostrado neste documento, caracteriza-se pôr ser uma ferramenta que localiza o ponto de acesso, trazendo informações sobre o qual, assim poderá ser utilizado também para identificar até que ponto as freqüências se limitam.

2.3.2 Decoy Device – Honeypots

Esta é uma técnica que tenta "iludir", para desestimular e dificultar as ações de prováveis invasores. A idéia é colocar vários equipamentos que irão transmitir informações falsas sobre redes *wireless* inexistentes, como o SSID, por exemplo. A identificação da verdadeira rede wireless utilizada torna-se uma tarefa mais complexa.

2.3.3 Desabilitar o Broadcast do SSID

Todos os pontos de acesso programam o SSID em *broadcast* para que os clientes tenham facilidade ao obter o acesso à rede. O detalhe é que o SSID não é criptogafado pelo o WEP e assim fica muito fácil para que o invasor possa obter informações importantíssimas para conseguir seu objetivo. Alguns concentradores permitem desabilitar a difusão da informação de SSID (*broadcast* SSID), desta maneira, apenas clientes com conhecimento prévio de dados como SSID e canal poderão estabelecer conexão.

Pode também ser útil mudar o nome SSID, escolher nomes que façam referência à organização ou empresa pode ser perigoso, assim, um possível atacante terá mais facilidade em identificar alvos específicos.

2.3.4 VPN – Rede Privada Virtual

As VPN (*Virtual Private Network),* são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos. Esta técnica, também chamada de tunelamento, cria “túneis virtuais” de comunicação entre dois pontos evitando "grampos" dos dados de uma rede corporativa (remota), desde a saída dos dados do *firewall* de um determinado ponto de presença (matriz), até a chegada no outro *firewall* de um outro determinado ponto de presença (filial).

O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e descriptografado, retornando ao seu formato original.

Além da criptografia, as VPNs oferecem a autenticação dos usuários, outro item de muita importância quando se trata de segurança no tráfego de dados, é

feita uma verificação na identidade do usuário através de um *login* e senha, por exemplo, e assim tenta restringir o acesso a pessoas autorizadas.

As VPNs podem se constituir numa alternativa segura para transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os *links* dedicados de longa distância, de alto custo, na conexão de WANs.

Entretanto, em aplicações onde o tempo de transmissão é crítico, o uso de VPNs através de redes externas ainda deve ser analisado com muito cuidado, pois podem ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos (HENTHORN, 2003).

2.3.5 Firewall

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre o computador e a Internet ou entre uma rede e a Internet. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. É um mecanismo que atua como "defesa", controlando o acesso de ambos os lados por meio das regras de sua configuração.

O *firewall* também pode assumir o papel de *gateway* entre duas redes, podendo estas redes ser uma WI-FI e a outra LAN (*Local Área Network*), desta forma é possível isolar as duas redes, evitando que pessoas não autorizadas que possuem acesso a uma rede, não tenha o mesmo privilégio em acessar a outra, bloqueando como desejado o tráfego que ocorre do lado WI-FI para a LAN e da LAN para WI-FI.

Existem duas formas de filtragem de tráfego:

a) Filtragem de pacotes: Este tipo se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP (*Internet Protocol*) remoto, endereço IP do destinatário, além da porta TCP (*Transmission Control Protocol*) usada.

Um *firewall* assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.

b) Filtragem de aplicação: Este tipo de *firewall* é mais complexo, porém muito seguro, pois todas as aplicações precisam de um *proxy* (exemplos de aplicação: SMTP, FTP, HTTP, etc). Este tipo não permite comunicação direta entre a rede e a Internet tudo deve passar pelo *firewall*, que atua como um intermediador. O *proxy* efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Isso não impede que pessoas que estão no mesmo lado da rede, seja a WI-FI quanto a LAN, possa de alguma forma, adquirir acesso a documentos que estejam compartilhados, segundo (ROSS, 2003).

2.3.6 WPA

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), o WPA surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, combatendo algumas das vulnerabilidades do WEP.

Para obter bons benefícios do com o protocolo WPA, e preciso o uso simultâneo de autenticação. Com o trabalho junto desses dois protocolos, é possível obter uma administração e um controle de acesso centraliza de toda a rede. Com isto, a necessidade de soluções adicionais como VPN pode ser eliminada, pelo menos, no que se diz respeito à segurança.

Apesar de não ser o padrão IEEE 802.11i ainda, é baseado neste e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente. Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado, sendo que para essa migração se requer um *upgrade* de *firmware*. Possui a compatibilidade com o 802.11i do futuro, com o propósito de evitar que seus usuários tenham que renovar os equipamento para se adaptar ao novo padrão. Este protocolo será detalhado no terceiro capítulo.

3 PROTOCOLOS DE SEGURANÇA (WEP E WPA)

3.1 WEP (*Wired Equivalent Privacy*)

Para que as redes *wireless* possam ser implementadas em ambientes corporativos, o IEEE 802.11b define a implementação de um protocolo de segurança denominado WEP, que atua com criptografia e autenticação na camada de enlace, entre as estações e o ponto de acesso. O WEP é simétrico, uma vez que usa chaves compartilhadas e estas chaves devem ser as mesmas no cliente e no ponto de acesso.

O WEP é baseado em um processo criptográfico RC4. Ele emprega uma chave secreta de 40 ou 104 bits que é compartilhada entre os clientes e o ponto de acesso da rede. Durante a transmissão do pacote, um IV (vetor de inicialização) de 24 bits é escolhido randomicamente e é anexado à chave WEP para formar uma nova chave de 64 ou 128 bits (MARTINS, 2003).

3.1.1 Objetivos do Protocolo

Em primeiro lugar, aparece a confidencialidade, tendo como objetivo, a garantia que o protocolo de segurança será capaz de evitar que um “intruso” (qualquer pessoa não autorizada a participar da comunicação) possa ler, remover ou inserir dados na rede.

Além de confidencialidade, o protocolo deve garantir aos seus usuários autenticidade e, para tal, deve implementar um controle de acesso a infraestrutura da rede sem fio. Ao utilizar-se o protocolo WEP, tem-se a opção de poder simplesmente descartar todos os pacotes que não chegarem devidamente criptografados pelo WEP. Fazendo isso, pode-se garantir que apenas usuários que tenham uma chave de criptografia WEP possam fazer parte da comunicação. Dessa maneira, realiza-se um controle de acesso à rede e uma decorrente autenticação dos usuários.

Por último, o terceiro objetivo a ser alcançado pelo protocolo é a integridade dos dados transmitidos. Para que uma mensagem enviada chegue até seu destinatário de forma correta, sem alterações, o protocolo implementa uma função linear chamada de “*checksum*” para que o conteúdo da mensagem transmitida seja protegido e mantido inalterado ao longo da transmissão.

3.1.2 Confidencialidade

A confidencialidade impede que pessoas não autorizadas tenham acesso à informação. Sua implementação é opcional. Quando está ativada, cada estação tem uma chave secreta compartilhada com o ponto de acesso, e não há uma forma padrão de distribuição dessas senhas, sendo feita manualmente em cada estação.

A técnica de criptografia da chave secreta é baseada no algoritmo RC4, projetado por Ronald Rivest em 1987. O RC4 é um algoritmo de fluxo, isto é, o algoritmo criptografa os dados à medida que eles são transmitidos, aumentando assim o seu desempenho. A lógica do algoritmo se manteve secreta até vazar e ser publicada na Internet em 2001 (ANDRADE, 2004).

Para enviar uma mensagem, a estação transmissora, inicialmente, concatena a sua chave secreta (*shared key*) a um vetor de inicialização (IV). O resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios (PRNG), definido pelo RC4. O PRNG (*Pseudo Random Number Generator*) gera uma seqüência de bits do mesmo tamanho que a informação a ser cifrada, ou seja, o *frame* MAC incluindo o CRC (*Cyclic Redundancy Check*) (Gast, 2002). Um XOR (OU exclusivo) é realizado entre o *frame* e a sequência de *bits*, gerando o *frame* cifrado. Finalmente, o *frame* é enviado juntamente com o IV para que o receptor possa fazer o processo inverso (ANDRADE, 2004).

O WEP utiliza o IV de 24 bits para proteger a chave secreta utilizada no processo de criptografia. A cada frame enviado, o IV é gerado e concatenado à chave secreta, fazendo com que a chave utilizada no ciframento do *frame* (*keystream*) mude a cada novo *frame* (MAIA, 2004). Porém, quanto maior o tamanho da chave criptográfica, mais seguro é o processo de criptografia.

3.1.3 Integridade

A integridade garante que o receptor obtenha os dados corretos, ou seja, que não haja alterações nos *frames* enviados pelo transmissor, nem dados indesejados incluídos na transmissão ou removidos no meio do caminho. A integridade é implementada no WEP através do polinômio CRC-32 (*Cyclic Redundancy Check*), onde é adicionado um ICV (*Integrity Check Value*) para cada carga útil (MAIA, 2004).

3.1.4 Autenticidade

A autenticidade identifica quem está executando uma determinada ação, podendo assim fazer um controle de acesso aos recursos disponíveis. Essa autenticação pode ser feita de duas maneiras. A primeira é padrão, chamada de sistema aberto (*open system*) que apenas identifica cada ponto de acesso com seu SSID. Esta opção deve ser evitada, pois caso o mecanismo de criptografia esteja desabilitado, qualquer dispositivo poderá se comunicar com o ponto de

acesso, já que o SSID é transmitido pelo próprio ponto de acesso em intervalos de tempo pré-definidos, podendo ser facilmente capturado e utilizado para acesso indevido à rede.

A segunda opção de autenticação do WEP é baseada na chave compartilhada, que utiliza a técnica de *challenge-response*. Nela, somente a estação é autenticada, solicitando ao ponto de acesso a sua autenticação. O ponto de acesso, então, gera um número aleatório (*challenge*) e o envia para a estação, que o recebe e o criptografa com a utilização do algoritmo RC4, enviando-o de volta (*response*). O ponto de acesso descriptografa a resposta e a compara com o número enviado. Caso essa comparação seja positiva, o ponto de acesso envia para a estação uma mensagem confirmando o sucesso da autenticação (ANDRADE, 2004).

3.1.5 Estrutura do WEP

Inicialmente, cada uma das partes que desejam participar da comunicação deve possuir uma chave secreta k que será usada no processo de criptografia e no processo inverso também. Esta chave k será a mesma usada tanto para criptografar os dados a serem transmitidos como para recuperar os dados na recepção. O nome que se dá a este processo é criptografia simétrica, devido ao fato da chave ser única para os dois processos. É importante lembrar que a troca de chaves deve ser feita de maneira segura, se possível pessoalmente, para que a segurança não seja comprometida. Será mostrado mais adiante que essa

mesma chave k também é usada para autenticação, o que torna o protocolo um tanto quanto vulnerável neste aspecto (VERÍSSIMO, 2002).

Então, supõe-se o desejo de enviar uma mensagem M, que será transmitida através de uma WLAN, que utiliza o protocolo WEP. Primeiramente, essa mensagem será computada por um programa conhecido como "*checksum*", que é um algoritmo polinomial detector de erros aleatórios, que irá gerar um ICV (*Integrity Check Value*) para que na recepção, possa ser verificada a integridade da mensagem. Neste caso, o algoritmo utilizado para fazer esse controle é o CRC - 32. Ele irá gerar um ICV de 4 bytes que deve ser recuperado exatamente igual pelo receptor da mensagem M, caso contrário, a mensagem recebida será imediatamente considerada errada e será descartada. Portanto P = { M, c(M) }, onde ´P´ é a mensagem total enviada. É importante observarmos que o texto plano não depende da chave k, como se demonstra na figura 3.1 abaixo:
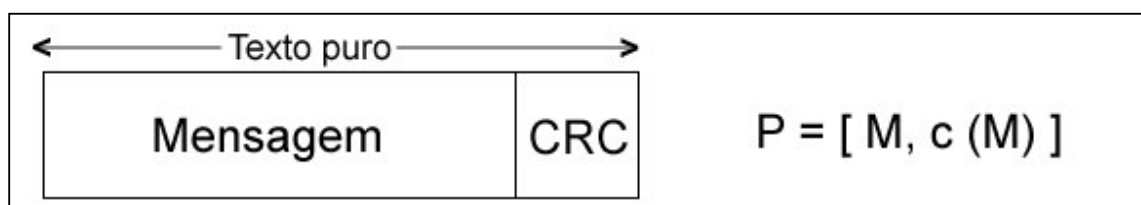
Figura 3.1 – Estrutura do Texto Plano

Num segundo estágio, é gerada uma seqüência de bits pseudo-aleatórios a partir da chave secreta k (40 bits) e de um vetor de inicialização IV (24 bits) gerado aleatoriamente também. Essa seqüência é gerada pelo algoritmo de criptografia RC4 e será indicada por RC4 (v,k).

Então, finalizando o processo de criptografia, faz-se um XOR entre o texto plano P e a seqüência RC4. O resultado dessa operação de XOR constituirá o pacote cifrado que será transmitido ao longo do ar. Esse pacote cifrado será aqui indicado por: C = P ⊗ RC4 (v, k), como na figura 3.2.
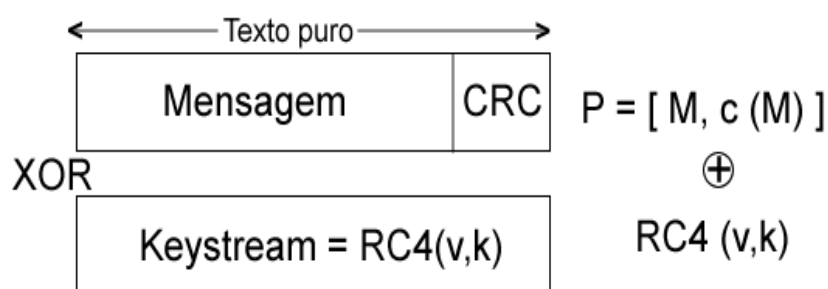
Figura 3.2 – Cenário para Pacote Cifrado

Além do pacote cifrado, transmite-se também o vetor de inicialização utilizado, para que o processo reverso de decriptar seja possível.

A recuperação do pacote se dá de maneira simples, aplicando-se o mesmo processo de maneira inversa. O receptor terá o pacote cifrado C e o vetor de inicialização v. Tendo-se este vetor e conhecendo-se a chave secreta k, o receptor pode utilizar o mesmo RC4 para gerar a seqüência de bits aleatória. Uma vez tendo essa seqüência, basta ele aplicar um XOR entre essa seqüência e o pacote cifrado para recuperar o texto plano P (pacote original). Isso só é possível devido a algumas propriedades do XOR que citaremos abaixo:

Na recepção, o receptor faz o processo inverso:

1) Com base em v (enviado junto de C) e em k (que ele já possui), é calculado o RC4.

2) É feito um XOR de RC4 com C:

$P' = C \oplus RC4(v,k)$

$P' = P \oplus RC4(v,k) \oplus RC4(v,k)$

$P' = P$

3) É calculado o *checksum* na forma [M´, c(M´)]. Se ele for igual a c(M), então M´= M

$P' = C \otimes RC4\ (v, k)$

$P' = (\ P \otimes RC4(v, k)\ ) \otimes RC4\ (v, k)$

$P' = P$

Então, fazendo-se o *XOR* da seqüência RC4 com ela mesma o resultado é zero. Portanto restará o *XOR* de uma seqüência de zeros com P. Mas, o resultado do *XOR* de qualquer número com zero, será o próprio número. Dessa maneira, foi possível recuperar o pacote original. O próximo passo do receptor agora será dividir o pacote em M´e c´(M´), em seguida ele recomputa o CRC-32 e compara o resultado obtido c(M´) com c´(M´). Se forem iguais, significa que o pacote recebido possui um *checksum* válido e portanto será aceito. Esta última etapa é realizada com o intuito de preservar a integridade dos dados transmitidos, fazendo com que o receptor rejeite pacotes que por ventura estejam corrompidos.

$C1 = P1 \otimes RC4(v,k)$

$C2 = P2 \otimes RC4(v,k)$

$C1 \otimes C2 = (P1 \otimes RC4(v,k)) \otimes (P2 \otimes RC4(v,k))$

$= P1 \otimes P2$

Ou seja, observa-se que com dois pacotes cifrados com a mesma seqüência, é possível recuperar um XOR dos dois textos planos sem conhecer a chave secreta e o vetor de inicialização. Isso só foi possível porque houve um cancelamento da seqüência RC4, que ocorreu devido ao fato dos dois pacotes terem sido igualmente cifrados. Esse resultado permite uma série de ataques ao protocolo, uma vez que se um dos dois textos é conhecido, imediatamente o outro torna-se conhecido. Mas conhecer um pacote não é tarefa tão difícil, afinal muitos pacotes possuem conteúdo previsível (ex: cabeçalho). Além disso, muitos textos possuem redundância, o que torna mais fácil descobrir seus conteúdos através de várias técnicas conhecidas. (ex: análise da frequência). A figura 3.3 a seguir ilustra o cenário com o transmissor e receptor:
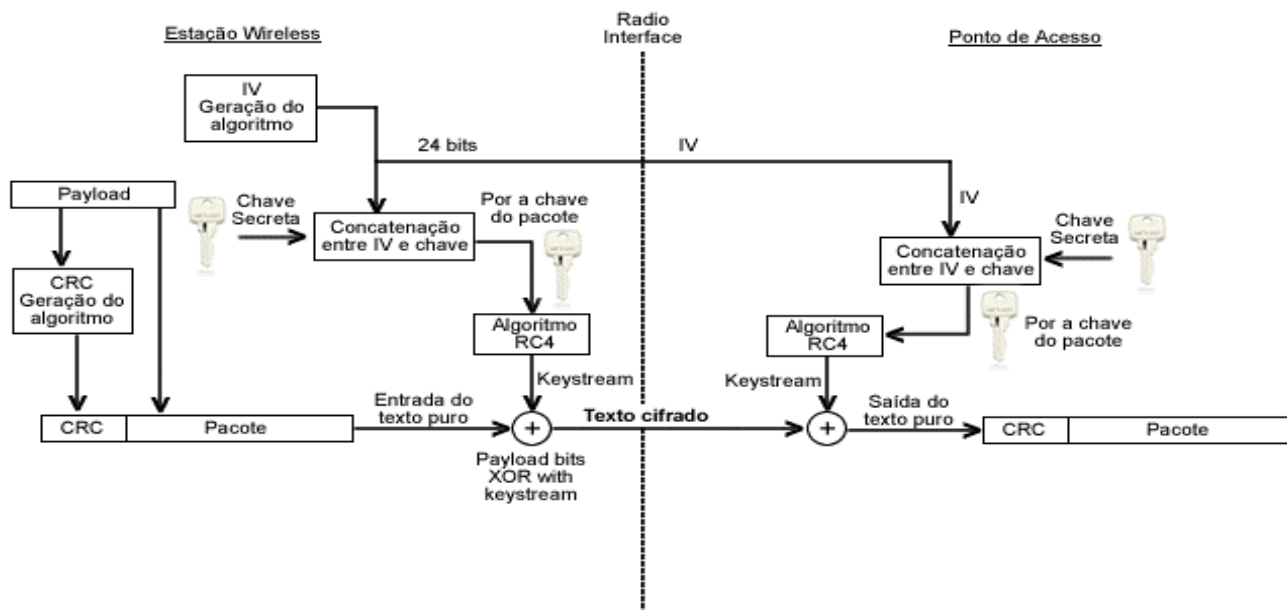
Figura 3.3 – Cenário para Transmissão entre Emissor e Receptor

3.1.6 Funcionamento da Autenticação

O usuário para poder fazer parte da rede sem fio, envia para o ponto de acesso um pedido de autenticação. Este retorna para o usuário uma espécie de desafio, ao qual o usuário deve cifrar utilizando o RC4 e a chave que ele possui, e então, enviar de volta o desafio cifrado para o ponto de acesso que vai utilizar a chave k para decifrar o conteúdo. Se o conteúdo recuperado pelo ponto de acesso for igual ao original, significa que o usuário utilizou a chave k correta e, portanto poderá ser autenticado e receberá uma confirmação do ponto de acesso.

No entanto, será mostrado que é possível violar a integridade dos dados, interceptando uma mensagem e modificando seu conteúdo. Isso só é possível

devido ao fato do *checksum* e do RC4 serem funções lineares. Suponha-se então que C é um texto cifrado capturado por um atacante malicioso que deseja inserir um ruído r no pacote. Então, ao inserir este ruído, o atacante modificará o texto cifrado C para C´da seguinte maneira:

$C' = C \otimes (r, c(r))$

$= RC4(v,k) \otimes (M,c(M)) \otimes (r, c(r))$

$= RC4(v,k) \otimes (M \otimes r,c(M) \otimes c(r))$

$= RC4(v,k) \otimes (M', \otimes c(M \otimes r))$

$= RC4(v,k) \otimes (M', \otimes c(M'))$

Portanto, fica provado a possibilidade de inserir um ruído numa mensagem alterando não só a mensagem original, como também o *checksum* da mensagem original, fazendo isso prova-se que o CRC-32 não foi capaz de manter a integridade dos dados.

3.1.7 Gerenciamento de Chaves

O padrão IEEE 802.11 não define como deve ser a distribuição das chaves. Ele é baseado num mecanismo externo de distribuição global da chave em um vetor de quatro chaves. Cada mensagem contém um campo de identificação de

chave que está sendo usada. Na prática, a maioria das instalações utiliza a mesma chave para todos os dispositivos.

Isso traz problemas profundos à segurança dessas instalações, uma vez que a chave é compartilhada com vários usuários, fica muito complicado manter o segredo. Alguns administradores de rede tentam amenizar o problema não revelando a chave secreta ao usuário final, configurando, eles mesmos, os dispositivos. Mas isso não traz a solução, pois as chaves continuam guardadas nos dispositivos remotos.

A reutilização de uma única chave por vários usuários também aumenta as chances da colisão do *IV*. A chance de uma colisão aleatória aumenta proporcionalmente ao número de usuários.

Uma vez que a troca de chaves requer que cada usuário reconfigure o seu dispositivo, as atualizações dos *drivers* controladores dos cartões de rede (NIC) serão cada vez mais infrequêntes. Na prática, a troca demorará meses ou anos para acontecer, dando mais tempo para intrusos analisarem o tráfego (VERISSIMO, 2002).

3.1.8 Reutilização do Vetor de Inicialização

O vetor de inicialização no WEP tem 24 bits, e junto com a chave, é o responsável por gerar a cadeia pseudo-aleatória que encripta o texto legível. O primeiro problema no WEP é justamente o tamanho desse IV que é muito

pequeno. No caso extremo, esse IV é alterado a cada pacote enviado, começando no zero e indo até o valor máximo (2²24)-1. Podemos calcular quanto tempo vai demorar para esse IV voltar a assumir o valor 0 novamente: imagine uma conexão cuja banda seja 5Mbits/s (o máximo no IEEE 802.11 é 11Mbits/s).

(5 *Mbits*/8)*1500 = 416 *pac/s*

(2^{23} *pac* /416) = 40.329 *seg* ou 11*h* 12*min*

Em suma, no caso mais extremo, numa conexão de 5Mbits/seg, o *IV* voltará a assumir o mesmo valor em menos de meio dia. Se a implementação assumir que o *IV* terá valores aleatórios teremos a repetição de *IV* em menos tempo. E é a partir dessa repetição de *IV* que o WEP pode ser quebrado. A chave K é fixa, e foi configurada nos clientes que estão se comunicando, logo o par <K,IV> repetir-se-á sempre que o *IV* se repetir. E sempre que eles se repetirem, gerarão a mesma string pseudo-aleatória, que iremos referenciar como RC4 (K,IV).

3.1.9 Vulnerabilidades

Apesar de o WEP ser bastante utilizado para tornar a comunicação de uma rede sem fio mais segura, muitas falhas são apontadas. Uma das vulnerabilidades desse protocolo está associada à reutilização do vetor de inicialização (IV).

Como dito, o IV possui 24 bits, podendo assumir valores entre 0 e 16M. Como são utilizadas as mesmas chaves por um longo período, o padrão WEP

recomenda que o IV seja alterado para cada pacote enviado, evitando assim a reutilização do fluxo de chaves. Normalmente, o IV começa do 0 e é incrementado de 1 a cada envio de pacote. Esse mecanismo tem dois problemas: o primeiro é que chegará um momento que o IV assumirá novamente o mesmo valor; e o segundo, reside no fato de que as pessoas, frequentemente, removem e reinserem os adaptadores de redes sem fio em seus computadores, fazendo com que o IV receba novamente o valor 0, tornando comuns os pacotes com IV com baixos valores.

Outra vulnerabilidade do WEP está relacionada ao CRC32. Como seu algoritmo de garantia de integridade é linear, possibilita que modificações sejam feitas no pacote sem que sejam detectadas. Apenas com o conhecimento da *string* de valores pseudo-aleatórias é possível alterar o conteúdo do pacote, não garantindo assim a integridade.

Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois o padrão WEP não especifica como deve ser a distribuição das chaves (VERÍSSIMO, 2002).

3.2 WPA (*Wi-Fi Protected Access*)

O WPA surgiu de um esforço conjunto de membros da *Wi-Fi* Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do

protocolo WEP. WPA pode ser definido ainda, como um subconjunto dos componentes 802.11i's. Usa o protocolo chave temporal do intercâmbio (TKIP), uma tecnologia mais segura de encriptação de chave do que RC4 de WEP (SANTOS, 2003).

Os seguintes recursos de segurança foram incorporados no WPA:

3.2.1 Forma de Autenticação

No WPA, é necessária a autenticação 802.1x. No padrão 802.11, essa autenticação era opcional. Para ambientes sem uma infra-estrutura RADIUS (*Remote Authentication Dial-In User Service*), WPA suporta o uso de uma chave pré-compartilhada. Para ambientes com uma infra-estrutura, EAP (*Extensible Authentication Protocol*) e RADIUS são suportados (Brian, 2003).

3.2.2 Administração da Chave do WPA

Com 802.1x, o *rekeying (*Troca de Chaves*)* das chaves de criptografia *unicast* é opcional. Além disso, 802.11 e 802.1x não fornecem mecanismos para alterar a chave de criptografia global usada para o tráfego *multicast* e *broadcast*. Com WPA, o *rekeying* das chaves de criptografia global e *unicast* é necessário. Para a chave de criptografia *unicast*, o TKIP (*Temporal Key Integrity Protocol*) altera a chave para cada frame, e a alteração é sincronizada entre o cliente e o

ponto de acesso. Para a chave de criptografia global, o WPA inclui um recurso para o ponto de acesso para avisar aos clientes conectados sobre a chave alterada (BRIAN, 2003).

3.2.3 TKIP

Para 802.11, a criptografia WEP é opcional. No WPA, a criptografia usando TKIP é necessária. TKIP substitui WEP por um novo algoritmo de criptografia mais forte do que o WEP, mas usa recursos de cálculo apresentados em dispositivos existentes para executar as operações de criptografia. TKIP também fornece o seguinte (MICROSOFT, 2004):

a) A verificação da configuração de segurança após as chaves de criptografia serem determinadas;

b) A alteração sincronizada da chave de criptografia *unicast* para cada quadro;

c) A determinação de uma única chave de criptografia *unicast* de partida para cada autenticação de chave pré-compartilhada.

3.2.4 Suporte ao AES

O WPA define o uso de AES (*Advanced Encryption Standard*) como uma substituição adicional da criptografia WEP. Como talvez não seja possível

agregar suporte AES por meio de uma atualização de *firmware* ao equipamento existente, o suporte a AES é opcional e depende do suporte ao *driver* do fornecedor.

3.2.5 Michael

Com 802.11 e WEP, a integridade dos dados é fornecida por um valor de verificação de integridade (ICV) de 32-bit que aparece com a carga útil 802.11 e é criptografado com WEP. Embora o ICV esteja criptografado, pode-se alterar os bits na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

Com WPA, um método conhecido como *Michael* especifica um novo algoritmo que calcula um código de integridade da mensagem (MIC) de 8 bytes usando os recursos de cálculo disponíveis nos dispositivos existentes. O MIC está localizado entre a parte de dados do quadro 802.11 do IEEE e o ICV de 4 bytes. O campo MIC é criptografado com os dados do quadro e o ICV.

O *michael* também fornece proteção a repetição. Para evitar ataques de repetição, é usado um novo contador de quadros no IEEE 802.11 (MICROSOFT, 2004).

3.2.6 802.11i & WPA & WEP

A tabela 3.1 abaixo faz uma comparação entre o WPA e o padrão que o mesmo antecede IEEE (*Institute of Electrical and Electronics Engineers)* 802.11i, é na tabela 3.2 a uma comparação entre os protocolos WEP E WPA.

Tabela 3.1 – Comparação entre 802.11b e WPA

	802.11i	**WPA**
SERVIÇOS BÁSICOS (BBS OU INFRAESTRUTURA)	SIM	SIM
BSS INDEPENDENTE (IBSS OU AD HOC)	SIM	SIM
PRÉ – AUTENTICAÇÃO	SIM	NÃO
HIERARQUIA DE CHAVE	SIM	NÃO
GERÊNCIA DE CHAVE	SIM	SIM
NEGOCIAÇÃO DA CRIFA DE AUTENTICAÇÃO	SIM	SIM
TKIP	SIM	SIM
AES – CCMP	SIM	NÃO

Tabela 3.2 – Comparação entre WEP e WPA

	WEP	**WPA**
“CIPHER”	RC4	RC4
TAMANHO DA CHAVE	40 BITS	128 BITS ENCRIPTAÇÃO 64 BITS AUTENTICAÇÃO
“KEY LIFE”	24 – BITS IV	48/128 BITS IV
PACOTE DE CHAVE	CONCATENADA	MISTURANDO FUNÇÕES
INTEGRIDADE DOS DADOS	CRC – 32	MIC
INTEGRIDADE DO ENCABEÇAMENTO	NÃO POSSUI	MIC

GERÊNCIAMENTO DE CHAVE	NÃO POSSUI	EAP – BASEADO

3.2.7 Como Utilizar WPA e WEP Juntos

Para suportar a transição gradual de redes com base em WEP para WPA, um ponto de acesso pode suportar clientes WEP e WPA ao mesmo tempo. Durante a associação, o ponto de acesso determina quais clientes usam WEP e quais usam WPA. A desvantagem do suporte a clientes WEP e WPA é o fato de a chave de criptografia global não ser dinâmica. Isso ocorre porque os clientes WEP não a suportam. Todos os demais benefícios aos clientes WPA, como a integridade, são mantidos. O WPA requer ainda as seguintes alterações nos softwares dos seguintes componentes:

a) Pontos de acesso sem fio.

b) Adaptadores de rede sem fio.

c) Programas de cliente sem fio

3.2.8 Vulnerabilidade

Uma pesquisa divulgada pelos laboratórios da ICSA Labs, uma empresa especialista em segurança revelou que o padrão *Wi-Fi Protected Access* (WPA) é menos seguro, em certas condições, que seu antecessor, o WEP. Na pesquisa denominada "Fraquezas Contundentes à Escolha da Interface WPA",

Robert Moskowitz, diretor sênior de tecnologia do ICSA Labs, parte da empresa TruSecure, descreve um número de problemas do novo padrão WPA, incluindo a possibilidade de invasores roubarem informações do tráfego *wireless* e descobrirem facilmente as senhas de redes sem fio.

Os problemas com o WPA se concentram no uso de *Pre-Shared Keys* (PSKs), uma ferramenta alternativa à autenticação, desenvolvida para pequenos negócios e usuários domésticos que não querem usar servidores de autenticação e infraestrutura 802.1x separados, de acordo com Moskowitz.

Moskowitz, que ajudou a desenvolver os padrões 802.11i e WPA de segurança wireless, relata que o método usado para os dispositivos WPA trocarem informações sobre encriptação de dados em redes *wireless* permite aos invasores que adivinhem a senha do PSK usando um ataque conhecido como “ataque dicionário”.

Nos "Ataques Dicionários", os invasores capturam o tráfico da rede *wireless* em trânsito entre pontos de acesso e estações de trabalho e usam programas específicos para adivinhar a senha. Outros padrões de segurança *wireless* também são vulneráveis aos ataques. A falha do WEP já é conhecida há tempos, mas, recentemente, foi provado que protocolo LEAP (*Lightweight Extensible Authentication Protocol*) de segurança, da Cisco, também é vulnerável a essas invasões.

O problema é que os invasores precisam pegar uma extensa quantidade de tráfego de rede nos padrões WEP e LEAP, enquanto no padrão WPA é necessário

apenas capturar quatro pacotes específicos de dados para decifrar as senhas, segundo Moskowitz, senhas com menos de 20 caracteres não resistem ao "Ataque Dicionário" e invasores que perderem os quatro pacotes podem facilmente efetuar um novo login e recebê-los de novo.
Uma saída, segundo Moskowitz, é usar senhas com mais de 17 caracteres. Empresas que usam servidores de autenticação não precisam se preocupar, já que não usam o PSK e, conseqüentemente, não sofrem riscos, de acordo com Michael Disabato, analista sênior do *The Burton Group*. Para ele, a pesquisa de Moskowitz não deve amedrontar os outros usuários."O WPA está fazendo o que tem que fazer".

Tanto Disabato quanto Moskowitz concordam que o padrão WPA é bem mais seguro que o WEP, mesmo com essas recentes falhas levantadas pela pesquisa. No entanto, Moskowitz revelou que o problema vem dos fabricantes de equipamentos e implementadores de WPA. Na pressa de oferecer o padrão WPA em seus produtos, os fabricantes, como o *Linksys Group* (agora conhecido como Cisco), fizeram muito pouco para previnir as falhas já conhecidas e informadas nos documentos oficias do padrão 802.11i.

3.3 Análise de Desempenho

3.3.1 Objetivos

Neste tópico será descrito os testes práticos realizados através da transferência de pacotes de dados com tamanhos variados. Este experimento foi realizado com intuito de demonstrar a variação do desempenho nas transferências de acordo com o método de criptografia utilizado, levando em consideração características como à taxa variável de transferências e tempo gasto para realizar as mesmas.

3.3.2 Experimentos

O experimento foi realizado com dois computadores, em uma distância de aproximadamente cinco metros do ponto de acesso (DWL 900AP+). Este ponto de acesso, está diretamente ligado na rede elétrica, sem nenhum cabo de rede ligado à ele, um dos micros funcionou como servidor de arquivos FTP, e o outro como cliente FTP, como representa a figura 3.4.

Figura 3.4 – Representação do Experimento.

Na tabela 3.3 abaixo, mostra - se a configuração das maquinas utilizadas no experimento.

Tabela 3.3 – Configuração dos Equipamentos

	SERVIDOR	CLIENTE
PROCESSADOR	ATHLON XP 2000 MHZ	ATHLON XP 2600 MHZ
PLACA MÃE	CHAINTECH 7KJD	ASUS
MEMORIA	SDRAM SANSUNG 256 MB	SDRAM SANSUNG 256 MB
DISCO RIGIDO	SANSUNG 40 GB 7200 RPM	SANSUNG 40 GB 7200 RPM
PLACA DE REDE WIRELESS	DWL 520 +AP	DWL 520 +AP

Neste experimento foram utilizados três tamanhos de arquivos diferentes: 52,6 MB, 271 MB e 692 MB. Cada um destes arquivos foi submetido a três transferências, sem criptografia, com criptografia WEP de 64 bits, com criptografia WEP de 128 bits e com criptografia WPA. Apartir destas três transferências foi estabelecida uma média, objetivando um resultado mais preciso.

A tabela 3.4 relata detalhadamente os experimentos realizados, no que diz respeito a taxas de transferência (Kbps) e a tabela 3.5 a tempo (segundos) adquiridas nos mesmos.

Tabela 3.4 – Taxa de Transferência

			TAXA DE TRANSFERENCIA			
EXPERIMENTO	**CRIPTOGRAFIA**	**TAM. DO ARQUIVO (BYTES)**	**1° Transf. (Kbps)**	**2° Transf. (Kbps)**	**3° Transf. (Kbps)**	**MÉDIA ENTRE AS TRANSFERÊNCIAS (Kbps)**
1	**NENHUMA**	55174894	505,9320	508,9930	498,4720	**504,4657**
2	**WEP 64**	55174894	470,1340	478,2180	480,3500	**476,2340**
3	**WEP 128**	55174894	479,4150	484,3980	484,5340	**482,7823**
4	**WPA**	55174894	499,2160	500,2540	498,7520	**499,4073**
5	**NENHUMA**	284858334	504,2530	505,8860	506,1450	**505,4280**
6	**WEP 64**	284858334	479,0050	477,3990	476,7730	**477,7257**
7	**WEP 128**	284858334	482,3660	485,3380	486,0800	**484,5947**
8	**WPA**	284858334	485,4570	484,5890	482,9020	**484,3160**
9	**NENHUMA**	725705726	479,4820	457,7180	486,9100	**474,7033**
10	**WEP 64**	725705726	485,2740	484,5640	484,0000	**484,6127**
11	**WEP 128**	725705726	469,1080	460,9970	467,8640	**465,9897**
12	**WPA**	725705726	471,2370	464,7790	467,2910	**467,7690**

Tabela 3.5 – Taxa de Tempo

			TAXA DE TEMPO			
EXPERIMENTO	**CRIPTOGRAFIA**	**TAM. DO ARQUIVO (BYTES)**	**1° Transf. (segundos)**	**2° Transf. (segundos)**	**3° Transf. (segundos)**	**MÉDIA ENTRE AS TRANSFERÊNCIAS (segundos)**
1	**NENHUMA**	55174894	106,5000	105,8590	108,0940	**106,8177**
2	**WEP 64**	55174894	114,6090	112,6720	112,1720	**113,1510**
3	**WEP 128**	55174894	112,3910	111,2340	111,2030	**111,6093**
4	**WPA**	55174894	108,4520	107,3340	109,8740	**108,5533**
5	**NENHUMA**	284858334	551,6720	549,8910	549,6090	**550,3907**
6	**WEP 64**	284858334	580,7500	582,7030	583,4690	**582,3073**
7	**WEP 128**	284858334	576,7030	573,1720	572,2970	**574,0573**
8	**WPA**	284858334	570,5130	571,3680	573,7210	**571,8673**
9	**NENHUMA**	725705726	1478,0470	1548,3280	1455,5000	**1493,9583**
10	**WEP 64**	725705726	1460,4060	1462,5470	1464,2500	**1462,4010**
11	**WEP 128**	725705726	1510,7340	1537,3130	1514,7500	**1520,9323**
12	**WPA**	725705726	1508,2870	1519,1180	1515,3500	**1514,2517**

3.3.3 Resultados

Apartir dos resultados obtidos com os experimentos, pode-se perceber que a qualidade do equipamento utilizado é pouca, por isso ele deixa a desejar, não superando taxas de transferência de 1Mbps, e mesmo equipamentos de melhor qualidade, como o Cisco, não superam os 4Mbps de taxa real de transferência.

Os gráficos a seguir, demonstram o experimento realizado com o arquivo de 52,6 MB. No gráfico 3.1, é apresentado uma comparação entre os diferentes valores de tempos de transferência (segundos) para cada processo, sendo este arquivo transferido sem criptografia, com criptografia WEP 64 e 128 bits e WPA. E no gráfico 3.2 é apresentado a comparação entre os diferentes valores de taxas de transferência (Kbps) para cada processo, usando os mesmos modelos de criptografia que o gráfico 3.1.
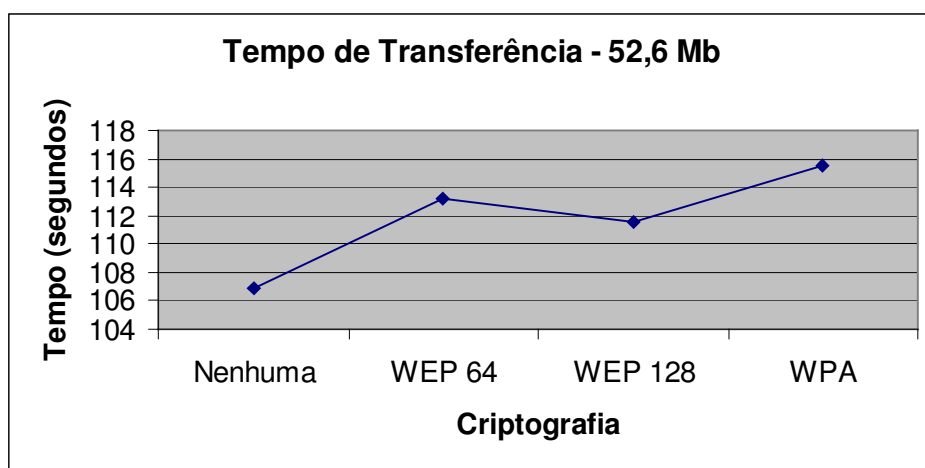
Gráfico 3.1 – Comparação de Tempos de Transferência para Arquivo de 52,6 MB.
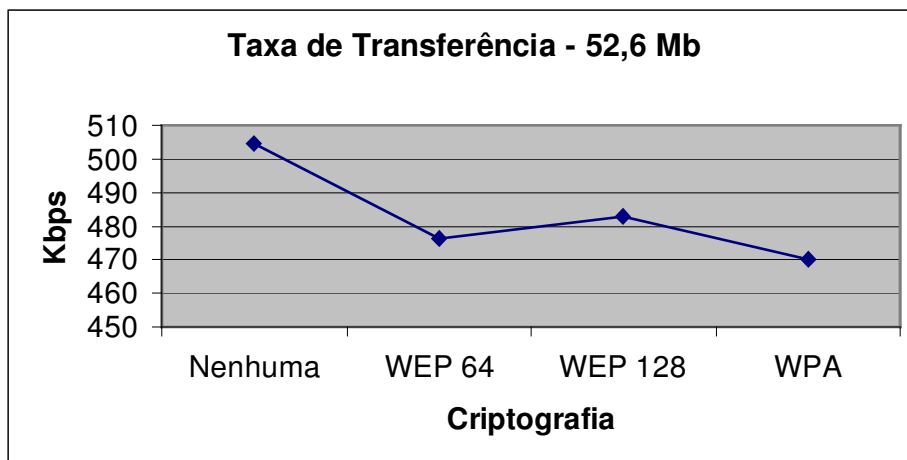
Gráfico 3.2 – Comparação da Taxa de Transferência para Arquivo de 52,6 MB

No gráfico 3.3, é apresentado uma comparação entre os diferentes valores de tempos de transferência (segundos) para cada processo, sendo este arquivo transferido sem criptografia, com criptografia WEP 64 e 128 bits e WPA. E no gráfico 3.4 é apresentado a comparação entre os diferentes valores de taxas de transferência (Kbps) para cada processo com a mesma criptografia acima.
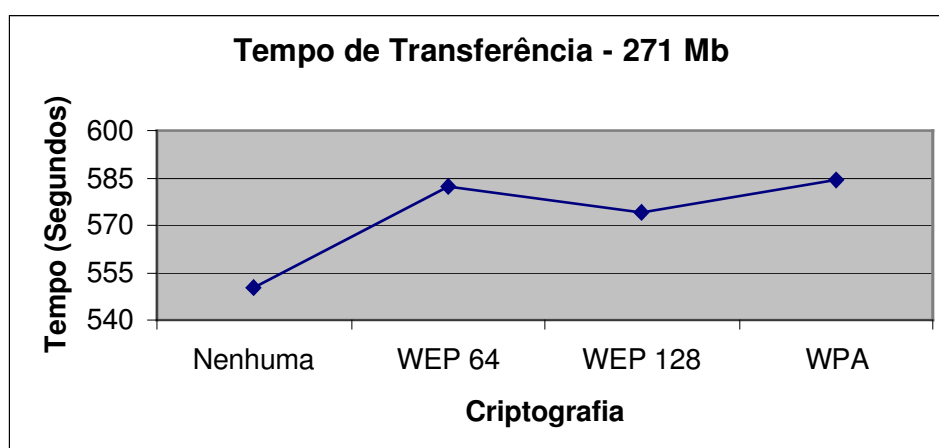
Gráfico 3.3 – Comparação do Tempo de Transferência para arquivo de 271 MB
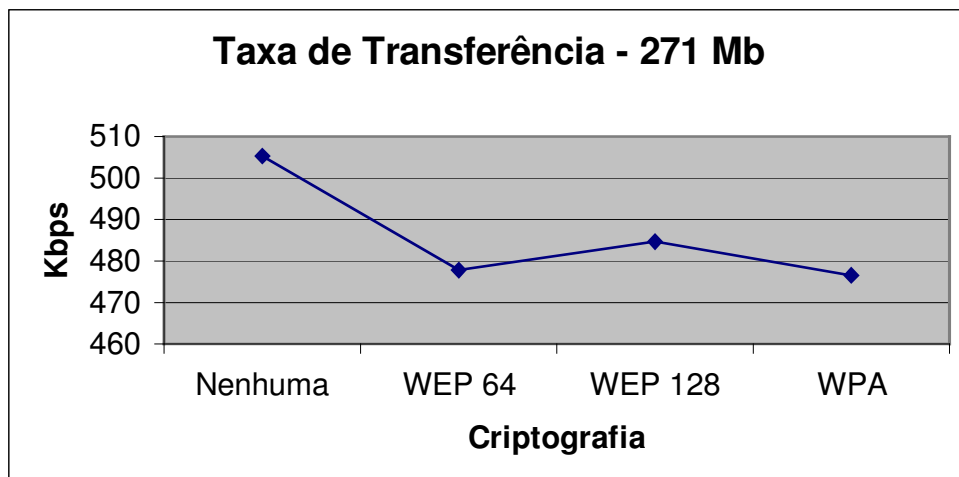
Gráfico 3.4 – Comparação da Taxa de Transferência para arquivo de 271 MB

No gráfico 3.5, é apresentado uma comparação entre os diferentes valores de tempos de transferência (segundos) para cada processo, sendo este arquivo transferido sem criptografia, com criptografia WEP 64 e 128 bits e WPA. E no gráfico 3.6 é apresentado a comparação entre os diferentes valores de taxas de transferência (Kbps) para cada processo com a mesma criptografia acima.
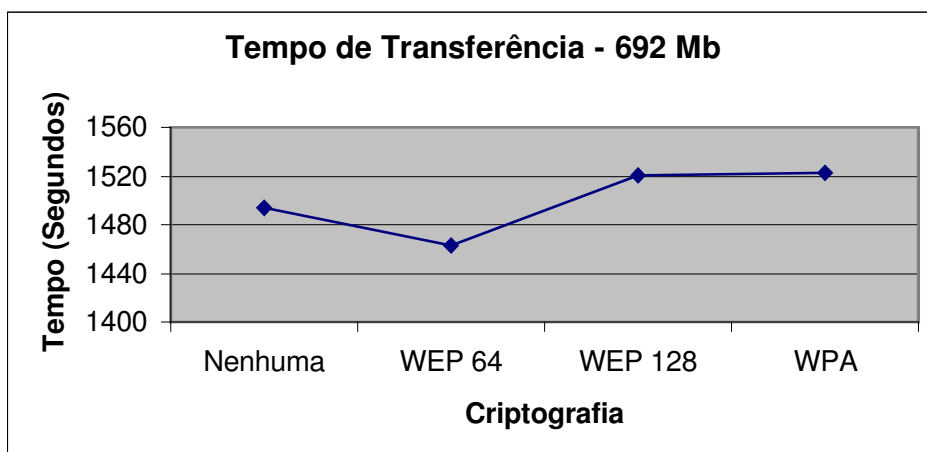
Gráfico 3.5 – Comparação do Tempo de Transferência para arquivo de 692 MB
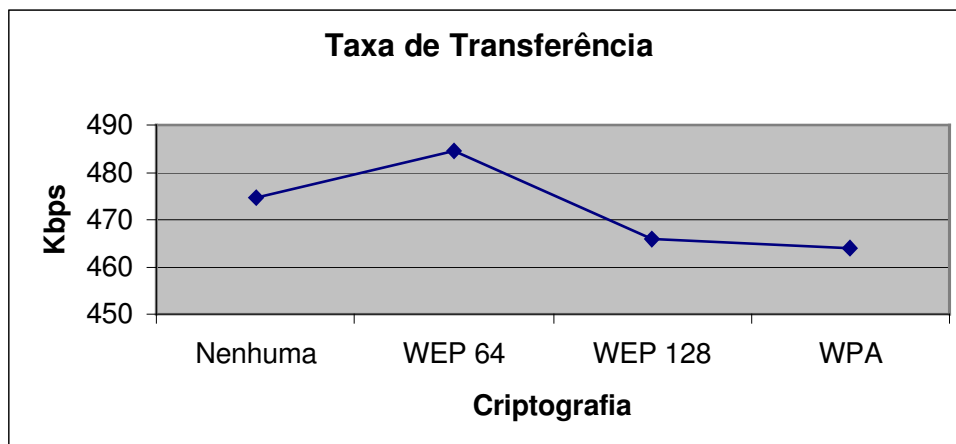
Gráfico 3.6 – Comparação da Taxa de Transferência para arquivo de 692 MB.

3.3.4 Conclusão

Os resultados obtidos no experimento não foram o esperado, pois, não se obteve uma seqüência lógica, sendo assim, os resultados deveriam mostrar que o tempo de transferência dos arquivos utilizando criptografia WEP 64 bits fossem menor do que a criptografia WEP de 128 bits e WPA que também utiliza 128 bits, porém isso só ocorre na transferência do arquivo de 692 MB. A seguir será feita uma análise de todos os gráficos, deixando claro que este estudo não explica o porque dessas taxas não terem obtido um resultado lógico.

Os gráficos 3.1 e 3.2 mostram que quando houve a transferência do arquivo de 52.6 MB sem nenhuma criptografia implementada o tempo e a taxa de transferência deste arquivo obedeceu à lógica, pois foi a transferência mais rápida neste caso. Já utilizando criptografia WEP de 64 bits o tempo de transferência subiu de forma inesperada, pois houve uma queda drástica na taxa de

transferência deste arquivo, chegando a ser ainda menor que a do protocolo WEP de 128 bits neste caso. Os resultados de WEP de 128 bits e WPA tiveram em seus resultados uma diferença de aproximadamente 4 segundos, não sendo uma diferença acentuada devido ao tamanho do arquivo que é pequeno, e a chave utilizada por ambos que é de 128 bits.

Os gráficos 3.3 e 3.4 mostram que quando houve a transferência do arquivo de 271 MB sem nenhuma criptografia implementada o tempo e a taxa de transferência deste arquivo ainda continuou obedecendo à lógica. Já utilizando criptografia WEP de 64 bits o tempo de transferência obteve o mesmo aumento inesperado em comparação ao demais protocolos.

Analisando os resultados obtidos na transferência do arquivo utilizando os protocolos WEP 128 bits e WPA, observou-se uma diferença acentuada, de aproximadamente 10 segundos. Este fato é explicado devido ao protocolo WPA possuir um reforço no seu algoritmo criptográfico, ou seja, além de utilizar 128 bits em seu processo de criptografia, este protocolo utiliza também um processo de segurança de autenticação, após estas chaves de criptografia serem determinadas, como conseqüência, ocorre o aumento do tempo de transferência.

Os gráficos 3.5 e 3.6 mostram que quando houve a transferência do arquivo de 692 MB sem nenhuma criptografia implementada, a lógica não se manteve, pois por motivos inexplicáveis, a taxa de transferência sem criptografia foi menor do que, quando utilizando criptografia WEP de 64 bits, logo, seu tempo de transferência aumentou de forma surpreendente. Quando se utilizou a

transferência do protocolo WEP de 64 bits, observou-se uma queda no seu tempo de transmissão, visto que tivemos um aumento relativamente grande da sua taxa de transferência. A partir daí constatou-se uma certa dúvida, pois este mesmo protocolo, obteve um desempenho muito menor nas transferências de outros arquivos menores, vistos nos resultados anteriores.

Comparando os resultados obtidos na transferência do arquivo utilizando os protocolos WEP 128 bits e WPA, nota-se uma certa aproximação de seus valores de transferência, sendo assim, seus tempos de transmissão ficam muito próximos da igualdade.

4 CONSIDERAÇÕES FINAIS

Este trabalho abordou os aspectos referentes ao que se considera hoje em dia a maior preocupação existente ao se tratar de redes sem fio: a segurança. Verificou–se que mobilidade e produtividade gerada pelas redes sem fio ainda não são capazes de superar as redes cabeadas, mas já começaram a ameaçá–las.

Também foi possível perceber que as redes wireless que utilizam o padrão IEEE 802.11b não representam um bom nível de segurança a seus usuários, pois seu principal protocolo de segurança, WEP, apresenta diversas vulnerabilidades. Mesmo com esforços feitos através dos fabricantes para conseguir suprir as falhas do WEP, com a criação de seu sucessor WPA, isso pouco surtiu feito, pois o WPA apenas representa uma dificuldade a mais para usuários mal–intencionados para explorar as fragilidades das WLANS, pois hoje em dia, já à falhas comprovadas com o uso do WPA.

Outro ponto demonstrado neste trabalho tem sua concentração na questão desempenho, no que se diz respeito ao uso de criptografia.

Foi demonstrado através de experimentos práticos que a utilização ou não de criptografia com os protocolos WEP e WPA, têm interferência direta no desempenho das transferências de dados para os usuários finais. Apesar de obter alguns resultados inesperados, ainda assim WEP 128 bits e WPA comportaram-se, em relação a desempenho, de forma equivalente, devido à utilização de ambos

da chave de 128 bits, ou seja, é aconselhável que utilize-se o protocolo WPA para garantir a autenticidade da chave, já que não há a perda de desempenho.

5 REFERENCIA BIBLIOGRAFICA

ANDRADE, Lidiane. “**Análise das Vulnerabilidades de Segurança Existentes na Redes Sem fio: Um estudo de caso do projeto WLACA**.” Jan.2004.

ARBAUGH, W. A. **“An inductive chosen plaintext attack against WEP/WEP2”**, IEEE. Document 802.11-01/230, May 2001.

BORISOV, N., GOLDBERG, I., and WAGNER, D. **“Intercepting Mobile Communications: Tha Insecurity of 802.11”,** Jan.2001.

BRIEN M. **“A segurança wireless de WPA oferece vantagens múltiplas sobre WEP”**, Set.2003. Disponível em: <http://216.239.37.104/translate_c?hl=pt-BR&ie=UTF8&oe=UTF8&langpair=en%7Cpt&u=http://techrepublic.com.com/5100-6265_5060773.html&prev=/language_tools> Acessado em: 15/10/2004.

FLUHRER, S. MANTIN, I. and SHAMIR, A., **“Weakness in the Key Scheduling Algorithm of RC4”**, Eighth Annual Workshop on Selected Areas in Cryptography, Ago. 2001.

GAUDÊNCIO, Mauricío. “**Quebrando barreiras. 2003. Artigo publicado no Telecom Negócios”**. Disponível em: <http://www.telecomweb.com.br/solutions/infraestrutura/segurança/artigo.asp?id=48566.>. Acessado em: 02/09/2004.

HENTHORN, A. **"VPN - Virtual Private Networks"** Livingston Enterprises, Inc. Disponível em: <http://www.cernet.com.br/Livingston/napl/vpn.htm.> Acessado em: 22/07/04.

HOUSLEY and WHITING, D. "**Temporal Key Hash", IEEE techical Report: IEEE 802.11-01/550r3.** "Disponível em: <http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-550.zip> Acessado em: 15/10/2004.

JOSHUA W. **"Detecting Wireless LAN MAC Address Spoofing"** Disponível em : <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf> Acessado em: 10/09/2004.

MARTINS, Marcelo. **"Protegendo Redes Wireless 802.11b."** Mar.2004.

PELISSON, A. **"Acesso ao meio** " Disponível em: <http://www.dainf.cefetpr.br/~pelisson/redes01b.htm> Acessado em: 19/08/2004.

IDG News Service **"Pesquisa Mostra Falhas em Padrão de Segurança Wireless"**, NOV.2004. Disponível em: <http://infobase.2it.com.br/?sec_cod=1&news_cod=245> Acessado em: 27/10/2004.

RIVEST, R. **"RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4", RSA Data Security"** Disponível em: <http://www.rsasecurity.com/rsalabs/technotes/wep.html> Acessado em: 15/10/2004.

SANTOS, C. IZABELA, **“WPA: A Evolução do WEP”**, Fev.2003. Disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos?id=70> Acessado em: 10/10/2004.

STUBBLEFIELD, Rubin, **“AT&T Labs Technical Report TD-4ZCPZZ”**, **“Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”**, Ago.2002.

MICROSOFT, **“Visão Geral da Atualização de Segurança WPA no Windows XP”**, MAR.2004. Disponível em: <http://support.microsoft.com/kb/815485/1> Acessado em: 15/10/2004.

VERISSIMO, F. **"Em defesa de Rivest", Lockabit”**, Dez.2001. Disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=55> Acessado em: 15/10/2004.

VERÍSSIMO, Fernando. **“Segurança em Redes sem fio.”** Disponível em: <http://www.projetoderedes.com.br/mono-2002.asp?id=0235.>. Acessado em 28/08/2004.

WALKER, J. R. **“Unsafe at any key size; an analysis of the WEP encapsulation”**, IEEE Document 802.11-00/362, Oct. 2000.